Aj	Authenticator of Terminal **J**	**L**	License, Certificate
Ao	Certificate Module	**Li**	License, Certificate issued to **I**
Bi	Token of User **I**	**LE**	Certificate of key **E**
Co	System Master Common Key	**LV**	Certificate of key **V**
Ci	Common Key of User **I**, symmetric key	**M**	Plaintext
Di	Private Decryption Key of User **I**, asymmetric key	**Mi**	Plaintext to or from User **I**
		Ni	ID# of User **I**
Ei	Public Encryption Key of User **I**	**NR**	Random Number
F	Unique Feature	**O**	System Authority
Fi	Unique Feature of User **I**	**P**	Ciphertext
F1	First Unique Feature (PIN/Password)	**Pi**	Ciphertext of User **I**
F2	Second Unique Feature (Biometrics)	**Qi**	Challenge Message sent to User **I**
G	Value of Mode Counter	**Ri**	Response Message from User **I**
G1	Value of Mode 1 Counter	**Si**	Signing Key of **I**
G2	Value of Mode 2 Counter	**So**	Signing Key of **O**
G3	Value of Mode 3 Counter	**TC**	Expiration Date of **Ci**
G4	Value of Mode 4 Counter	**TE**	Expiration Date of Certificate **LE**
H	Authentication Reference Hash Value of Unique Feature	**TL**	Logon Time
H1	Hash Value of PIN or Password **F1**	**TM**	Mode Expiration Period
H2	Feature Vector of Biometrics **F2**	**TP**	Present Time
I	User	**TV**	Expiration Date of Certificate **LV**
J	Local Terminal	**Ui**	Message Authorized by **I**, signed by **Si**
K	Key **C**, **D**, **E**, **S**, **V**	**Vi**	Verification key of **I**
K {M}	Cryptographic Operation **M** is encrypted by **K**	**Vo**	Verification key of **O**

FIG 1: Notation

(201) $\mathbf{P = K\{M\}}$ **M** is encrypted by **K**

(202) $\mathbf{M = K\{P\}}$ **P** is decrypted by **K**

(203) $\mathbf{TP - TL \leq TM}$

(204) $\mathbf{G > 0}$

(205) $\mathbf{Ci = Co\{Ni + TC\}}$

(207) $\mathbf{LEi = So\{Ni, Ei, TE\}}$

(208) $\mathbf{Vo\{LEi\} => Ni, Ei, TE}$

(209) $\mathbf{LVi = So\{Ni, Vi, TV\}}$

(210) $\mathbf{Vo\{LVi\} => Ni, Vi, TV}$

(211) $\mathbf{Qi = NR + TP}$

(212) or $\mathbf{Qi = Mi + TP}$

(213) $\mathbf{Ri = Ci\{Qi\}}$

(214) $\mathbf{Ci\{Ri\} => Qi}$

(215) $\mathbf{Ri = Di\{Qi\}}$

(216) $\mathbf{Ei\{Ri\} => Qi}$

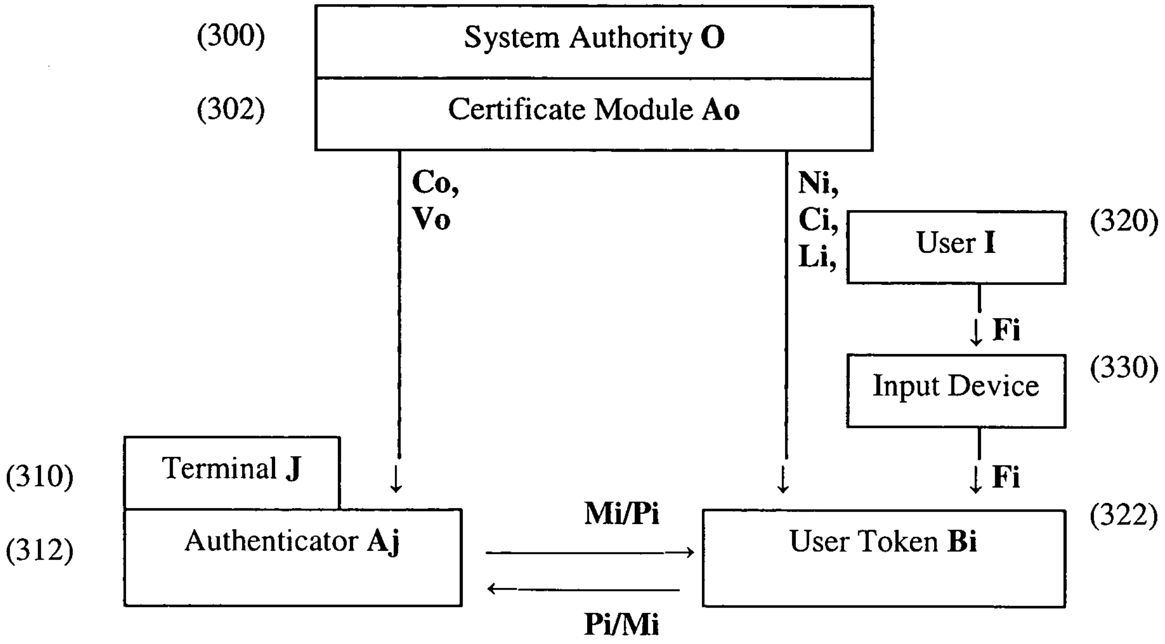
(217) $\mathbf{Pi = Ei\{Mi\}}$

(218) $\mathbf{Mi = Di\{Pi\}}$

(219) $\mathbf{Ui = Si\{Mi\}}$

(220) $\mathbf{Vi\{Ui\} => Mi}$

FIG 2: Formulae



Ci	Common Key of User **I**, symmetric key
Co	System Master Common Key
Fi	Unique Feature of User **I**
Li	License, Certificate issued to User **I**
Mi	Plaintext to or from User **I**
Ni	ID# of User **I**
Pi	Ciphertext of User **I**
Vo	Verification key of **O**

FIG 3: Block Diagram of the System of This Invention

Mode	Logon Expiration Period **TM**	Application Security Level
0	No Limit	No Security
1	1 week	Low
2	1 day	Middle
3	1 sign	High
4	1 sign	Highest

FIG 4: An Example of the Modes of a Multi-Mode Token

Register Name	Value in Register
Logon Time Register	**TL**
Mode 1 Counter	**G1**
Mode 1 Expiration Period	**TM1**
Mode 2 Counter	**G2**
Mode 2 Expiration Period	**TM2**
Mode 3 Counter	**G3**
Mode 4 Counter	**G4**

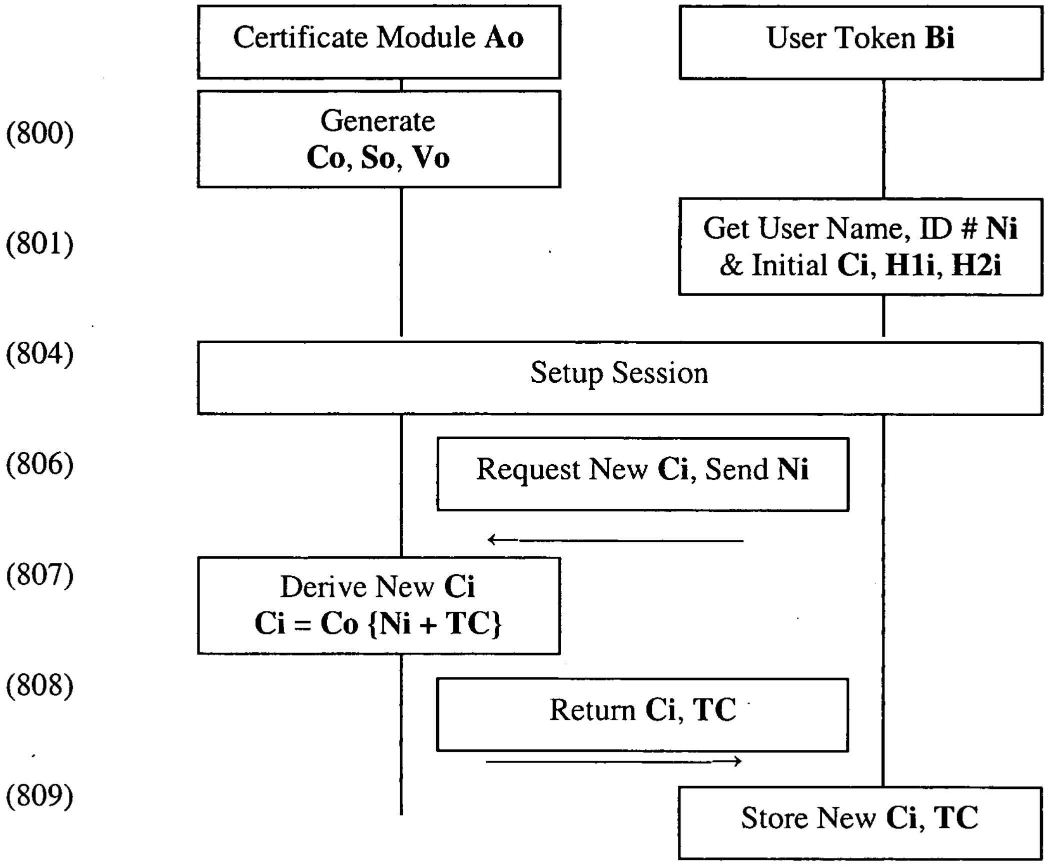
FIG 5: The Register & Counter values of a Multi-Mode Token

Item	Notation & Data	Secret
User Name		
Token ID #	**Ni**	
Common Key	**C**	X
Expiration Date of **C**	**TC**	
Private Decryption Key	**D**	X
Public Encryption Key	**E**	
Certificate of **Ei**	**LE**	
Expiration Date of **LE**	**TE**	
Private Signing Key	**S**	X
Public Verification Key	**V**	
Certificate of **V**	**LV**	
Expiration Date of **LV**	**TV**	
Public Verification Key of **O**	**Vo**	
Authentication Reference		
Hash Value of PIN or Password	**H1**	X
Feature Vector of Biometrics	**H2**	X

FIG 6: A Table of the Basic User Data Stored in a Multi-Mode Token

Mode	Crypt Key	Crypt Operand bit	Usage Condition			Application			
			Logon	Access Times G max	Expiration Period **TM**	Decrypt	Sign for		
							Authentication	Payment	Authorization
0	N/A	N/A	Free						
1	**C**	No Limit	**F1** or **F2**	10	1 week		Low		
2	**D**	< 1024	**F1** or **F2**	5	1 day	Session Key, File Key	High	Micro	
3	**S**	≤ 64	**F1** or **F2**	1	1 session			Regular	Regular
4	**S**	> 64	**F1** and **F2**	1	1 session			Large	Important

FIG 7: An Example of Multi-Mode Settings



Ci	Common Key of User **I**, symmetric key
Co	System Master Common Key
H1i	Hash Value of PIN or Password
H2i	Feature Vector of Biometrics
So	Signing Key of **O**
TC	Expiration Date of **Ci**
Vo	Verification Key of **O**
{ }	Cryptographic Operation

FIG 8A: Initialization Flow of Token

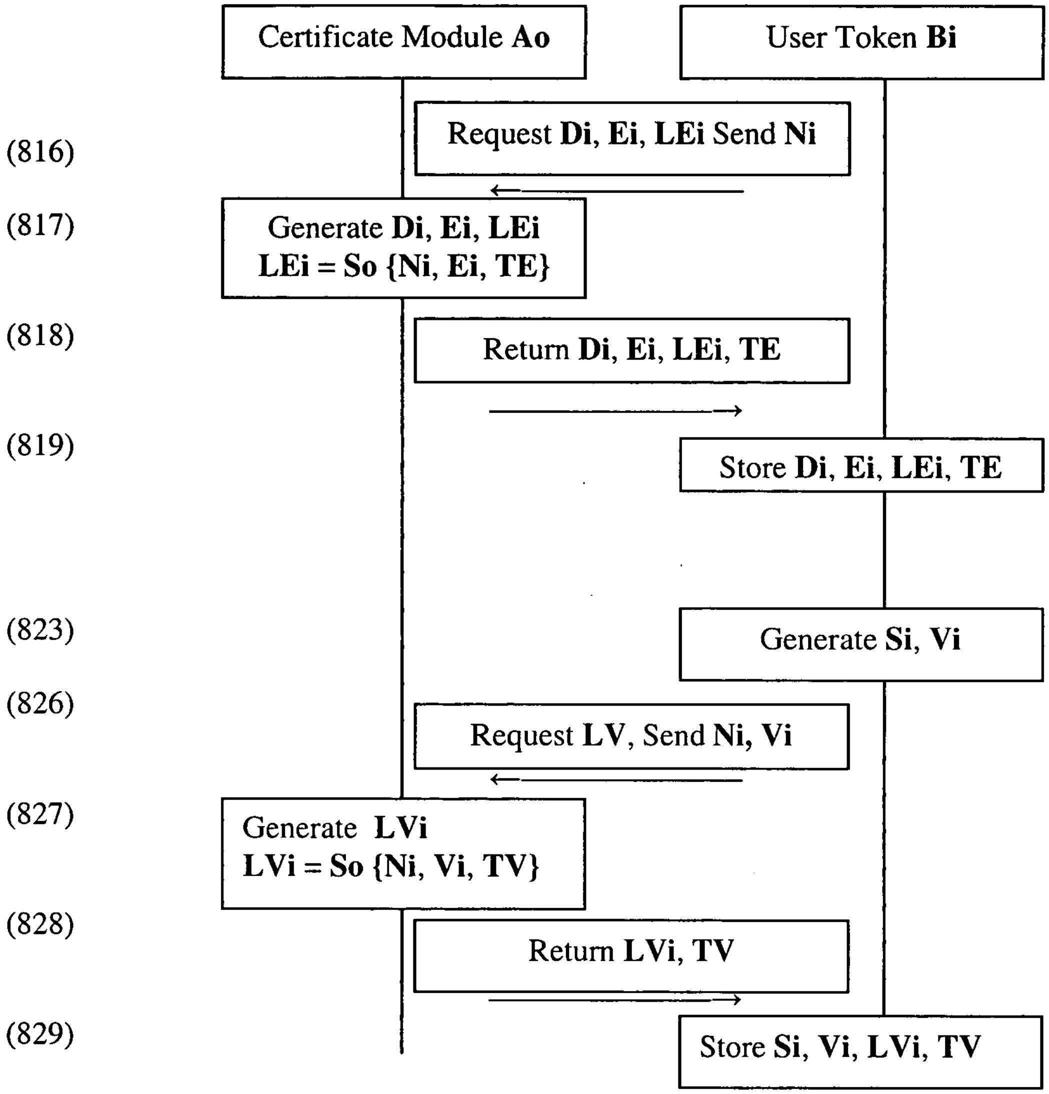

Certificate Module **Ao**
User Token **Bi**
(816)
Request **Di, Ei, LEi** Send **Ni**
(817)
Generate **Di, Ei, LEi**
LEi = So {Ni, Ei, TE}
(818)
Return **Di, Ei, LEi, TE**
(819)
Store **Di, Ei, LEi, TE**
(823)
Generate **Si, Vi**
(826)
Request **LV**, Send **Ni, Vi**
(827)
Generate **LVi**
LVi = So {Ni, Vi, TV}
(828)
Return **LVi, TV**
(829)
Store **Si, Vi, LVi, TV**

FIG 8B: Initialization Flow of a Token (continued)

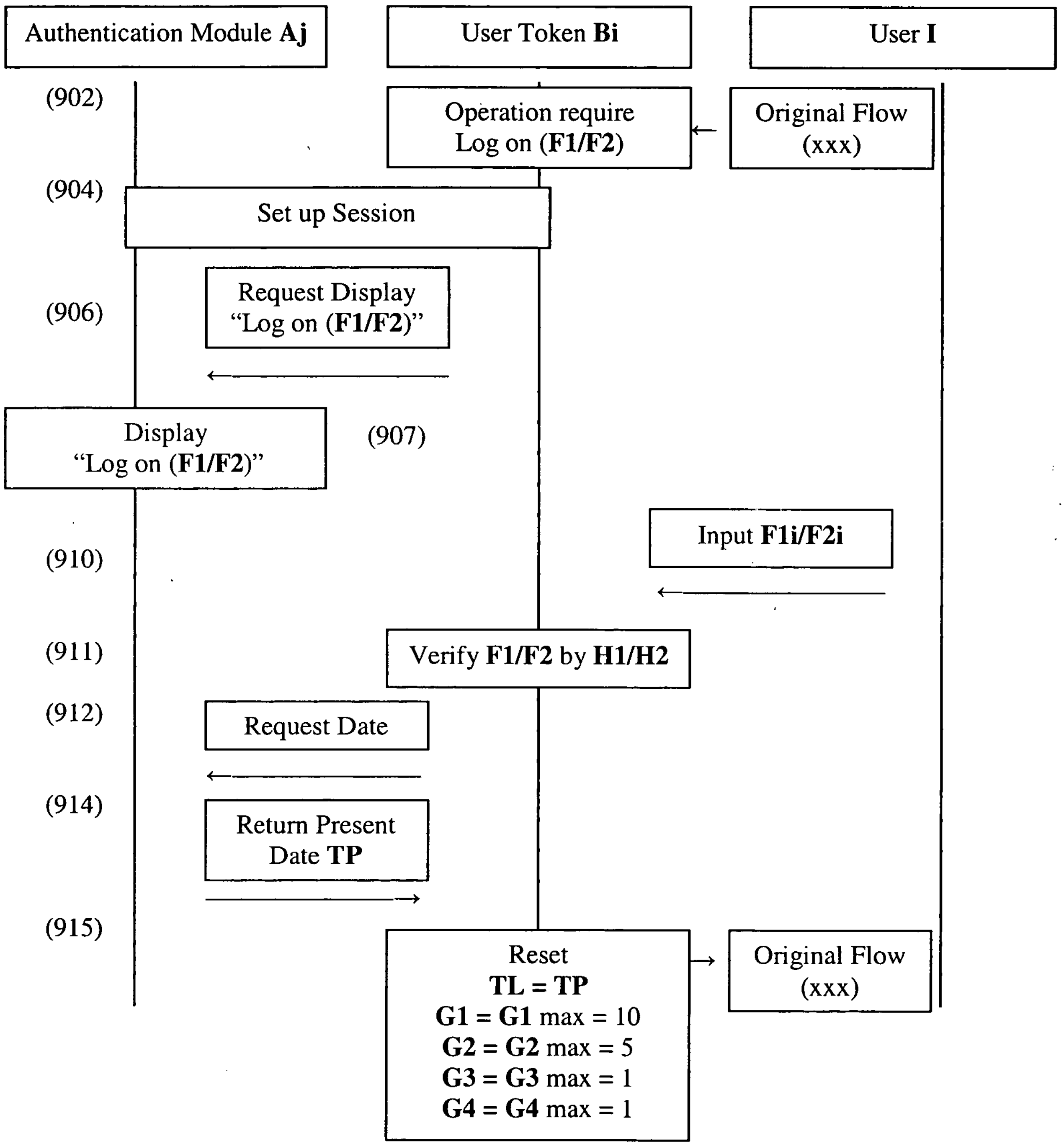


FIG 9: Flow of Multi-Mode Token Logon

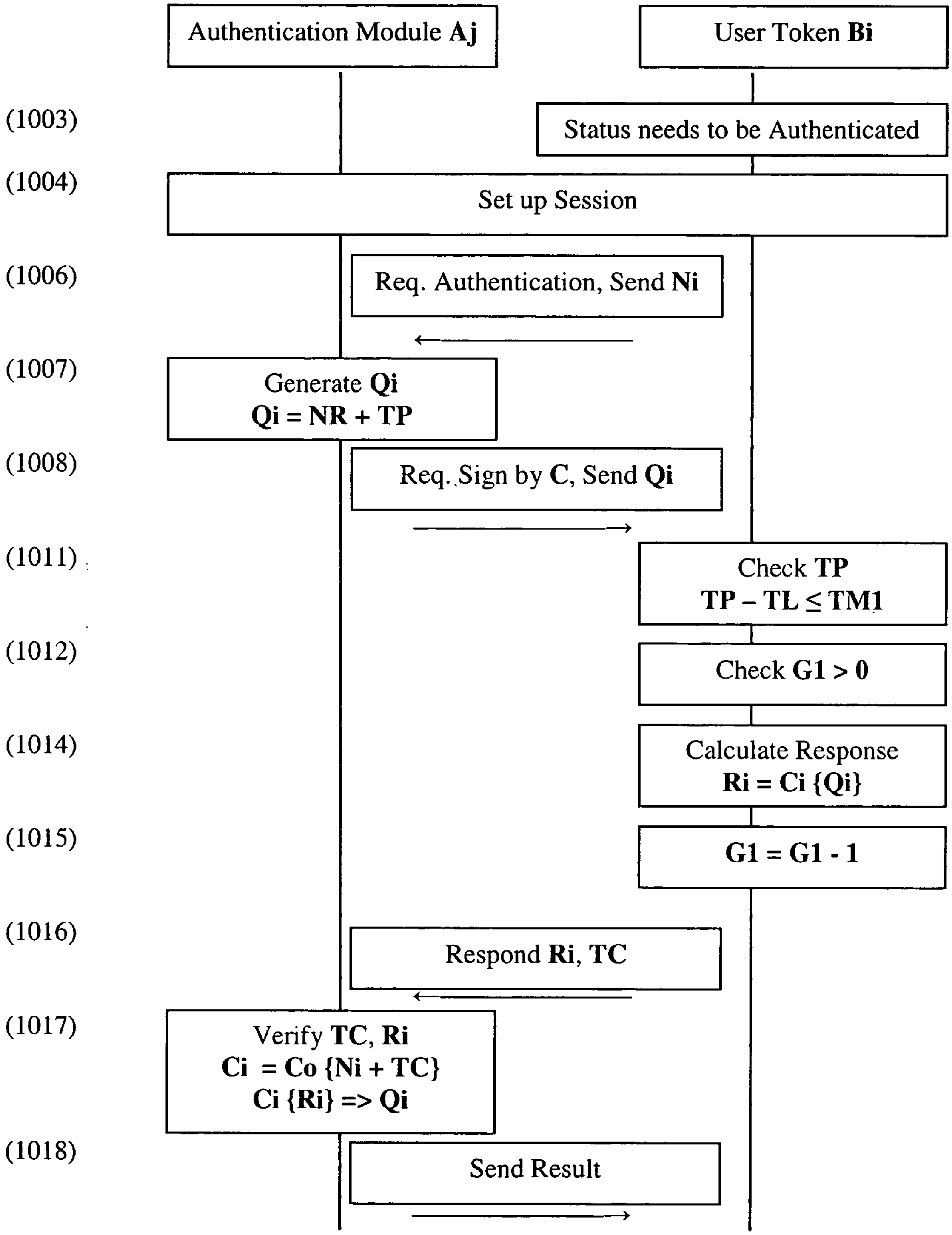


FIG 10: Flow of Mode 1 Operation

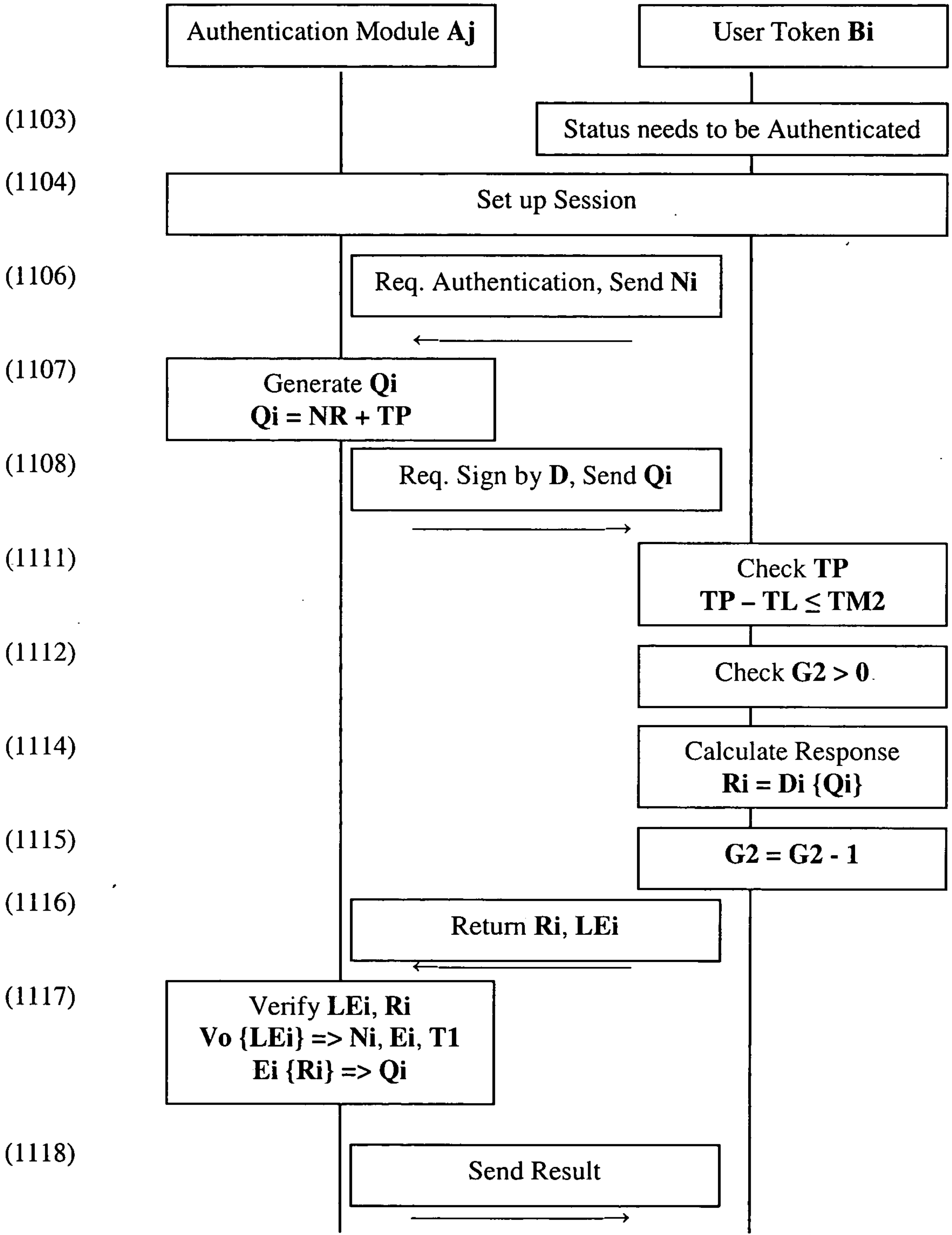


FIG 11: Flow of Mode 2, Authentication

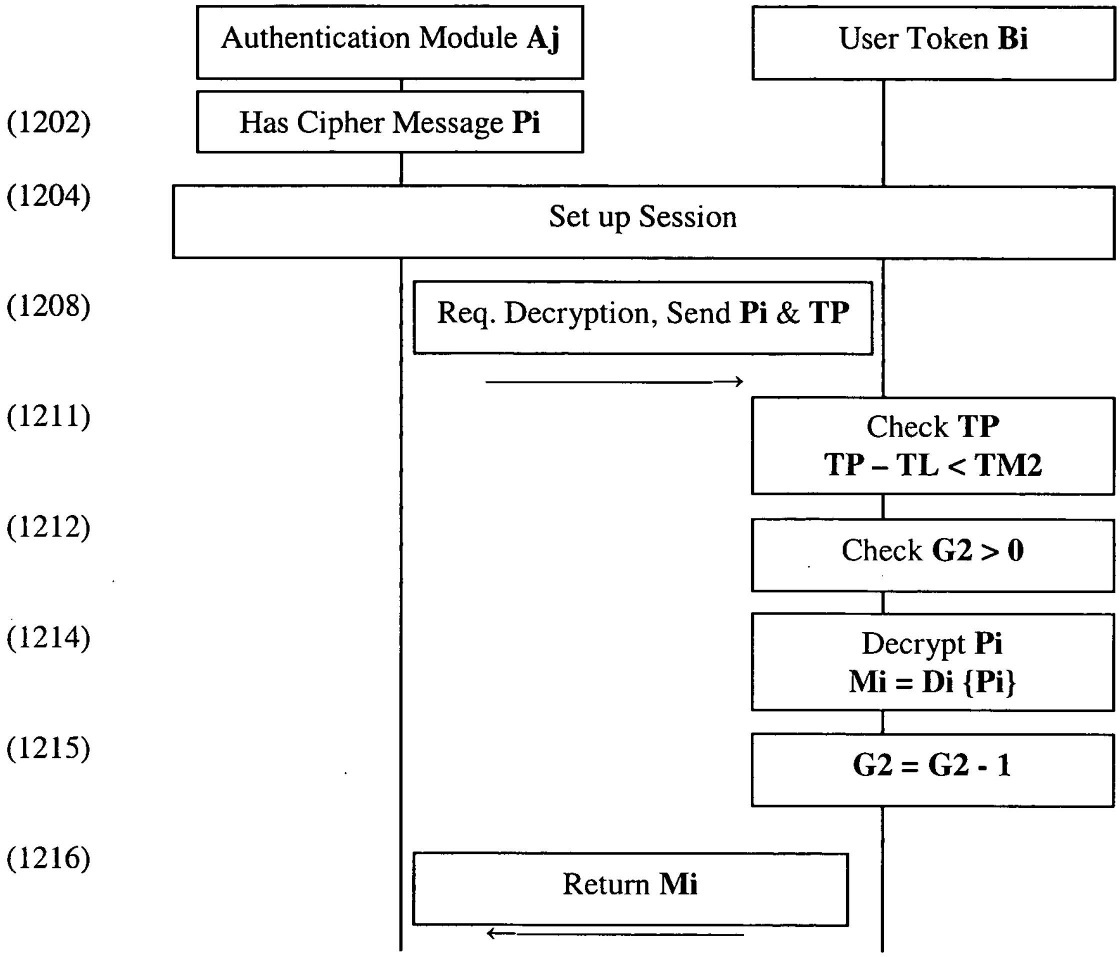


FIG 12: Flow of Mode 2, Decryption

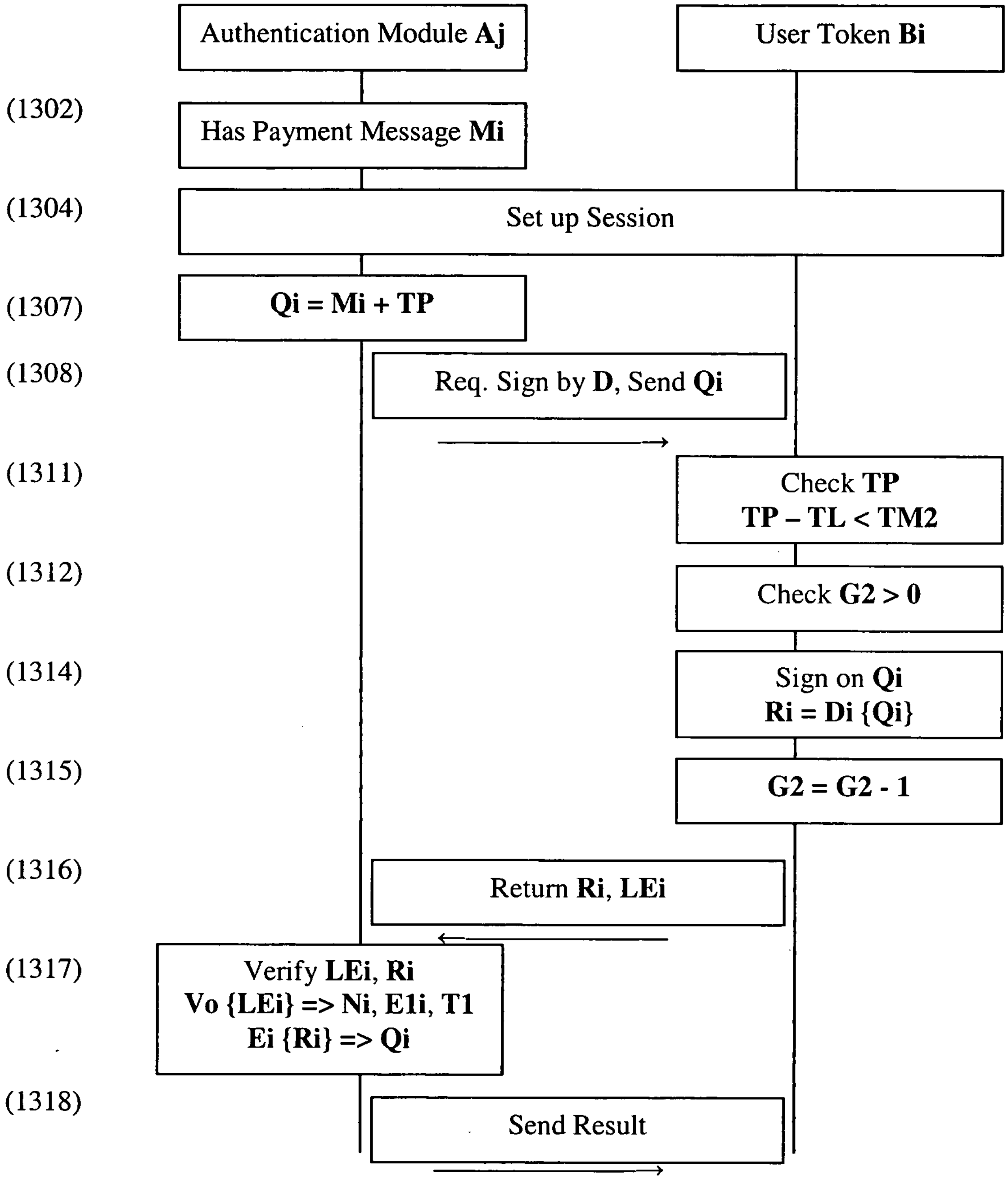


FIG 13: Flow of Mode 2, Payment

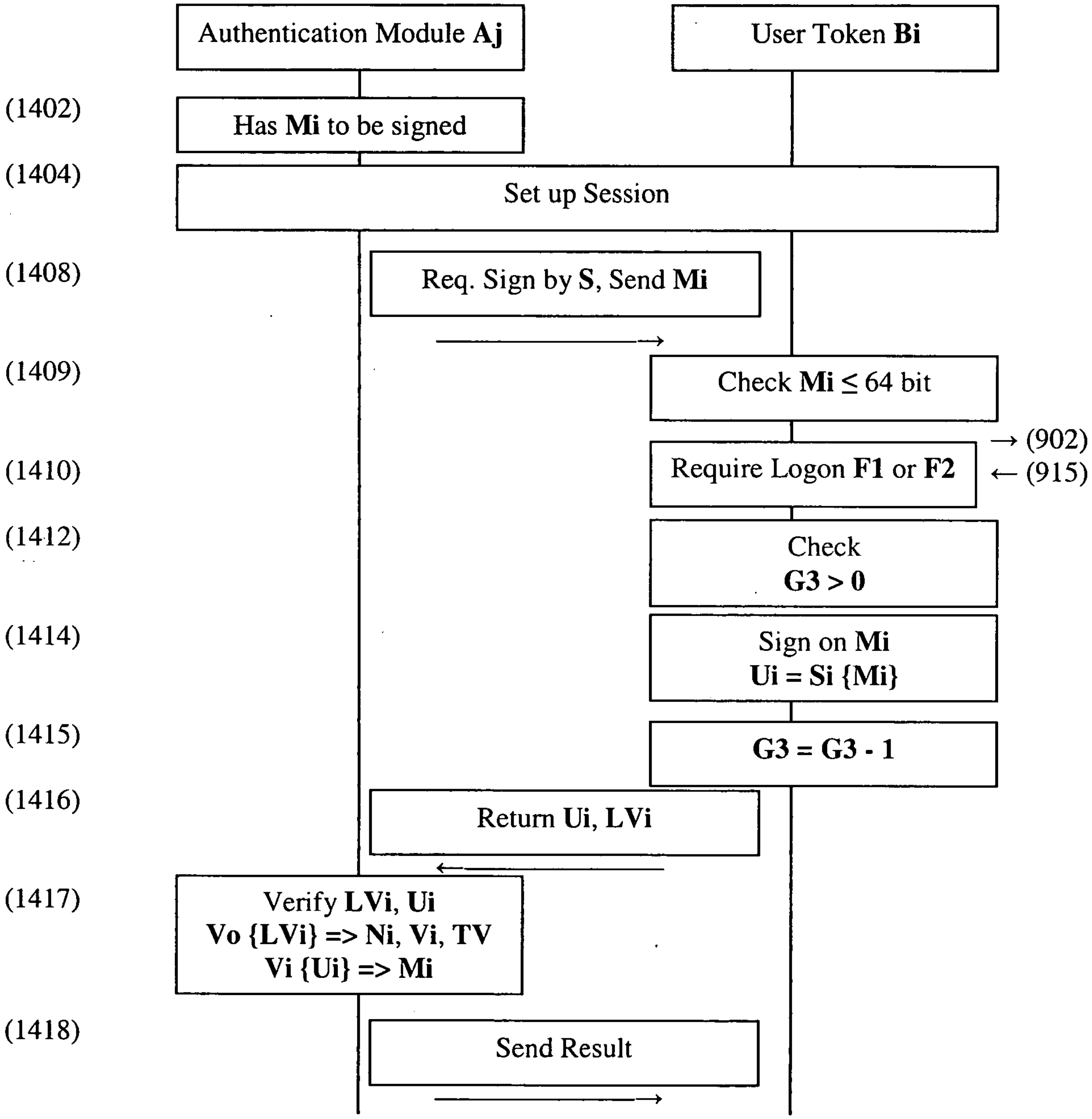


FIG 14: Flow of Mode 3 Payment/Authorization

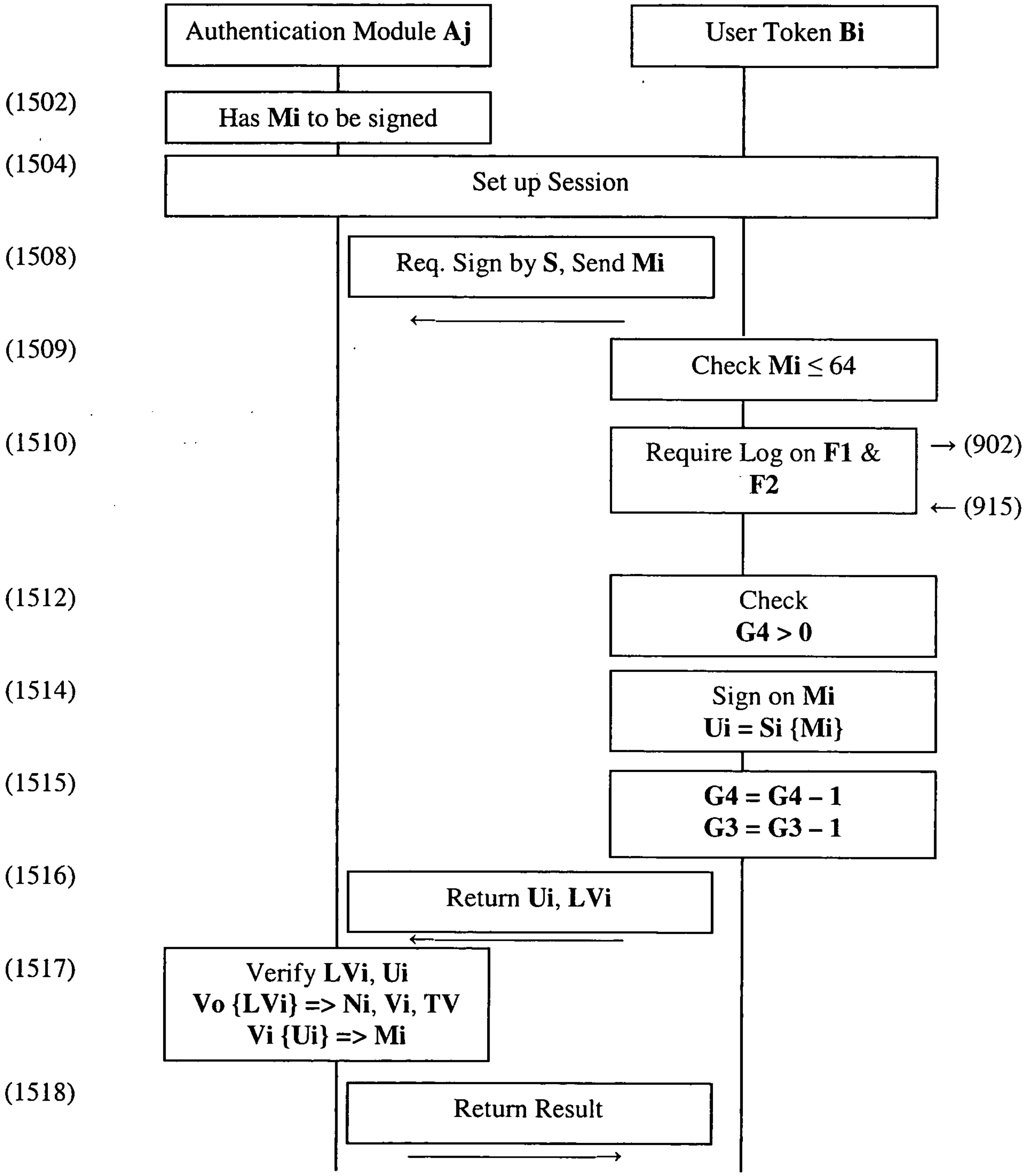


FIG 15: Flow of Mode 4 Payment/Authorization